Data Release Manual

Version 1.1

MARYLAND HEALTH CARE COMMISSION | https://mhcc.maryland.gov/

Table of Contents

Background

MHCC background

The Maryland Health Care Commission is an independent regulatory agency whose mission is to plan for health system needs, promote informed decision-making, increase accountability, and improve access in a rapidly changing health care environment by providing timely and accurate information on availability, cost, and quality of services to policy makers, purchasers, providers and the public.

The Commission's vision for Maryland is to ensure that informed consumers hold the health care system accountable and have access to affordable and appropriate health care services through programs that serve as models for the nation.

Data Available for Release

MDCB Data

The Maryland Health Care Commission (MHCC) is the Medical Care Data Base (MCDB) governing body. MHCC is responsible for all MCDB operations, including data submission compliance governed by COMAR 10.25.06 regulations, analysis, and reporting.

The MCDB is a large-scale database that collects and aggregates eligibility data, professional services claims, institutional services claims, pharmacy (prescription drug) claims, dental claims (limited to ACA-compliant plans), and provider data for Maryland residents and nonresidents (whose health insurance contracts were written or sold in Maryland), enrolled in privately insured health plans (approximately 34 reporting entities), Medicaid Managed Care Organizations (MCO), Medicaid Fee-For-Service (FFS), and Medicare FFS plans. The MCDB is Maryland's All-Payer Claims Database (APCD). As of 12/31/2020, the total covered lives (Maryland and Non-Maryland) in the MCDB is about 4.5 million consisting of 2.2 million for Commercial, 1.5 million for Medicaid (MCOs and FFS), and 780K for Medicare (Advantage and FFS).

Commercial Data

MHCC collects Commercial data quarterly from 34 privately insured reporting entities with at least 1,000 total covered lives and all qualified health and dental plans. All reporting entities submit claims and enrollment information to Onpoint Health Data, the MHCC's MCDB contractor. The private insurer health plans include multiple reporting entities from CareFirst, United Health Care, Kaiser Permanente, Aetna, and CIGNA and the major prescription benefit managers such as Caremark. Health plans with smaller market shares, such as Humana, also submit. A growing priority is the collection of Medicare Advantage claims, which are administered by private entities, including large health plans and several Medicaid MCOs, including Johns Hopkins.

Medicaid Data

MHCC receives Medicaid data through a DUA with Medicaid and includes this data in the MDCB. If an applicant requests Medicaid data, Commission staff will notify Medicaid in accordance with COMAR 10.25.05.04. Medicaid can choose to conduct its own review of the data request or defer to MHCC.

Medicare Data

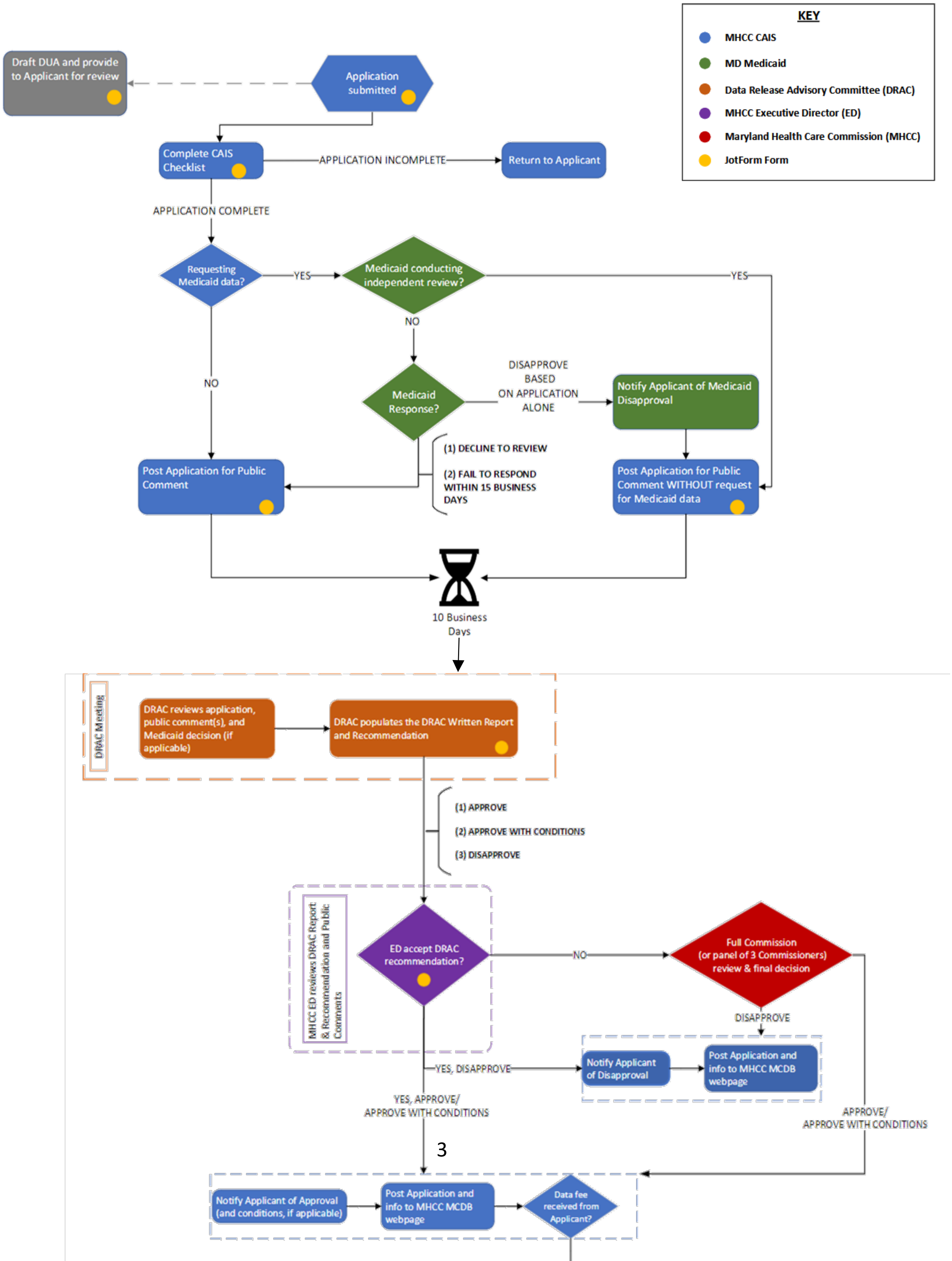
MHCC receives Medicare data from the Centers for Medicare & Medicaid Services (CMS). As described in CMS' State Data Request Memo dated June 2012, MHCC is the state agency that receives Medicare data from CMS for research activities on behalf of all Maryland agencies. Under the DUA that MHCC has entered into with CMS, MHCC is permitted to re-disclose the data with other State agencies for research purposes on behalf of the State. This data is therefore only available for release to other State agencies.

Composition of the Data Release Advisory Committee (DRAC)

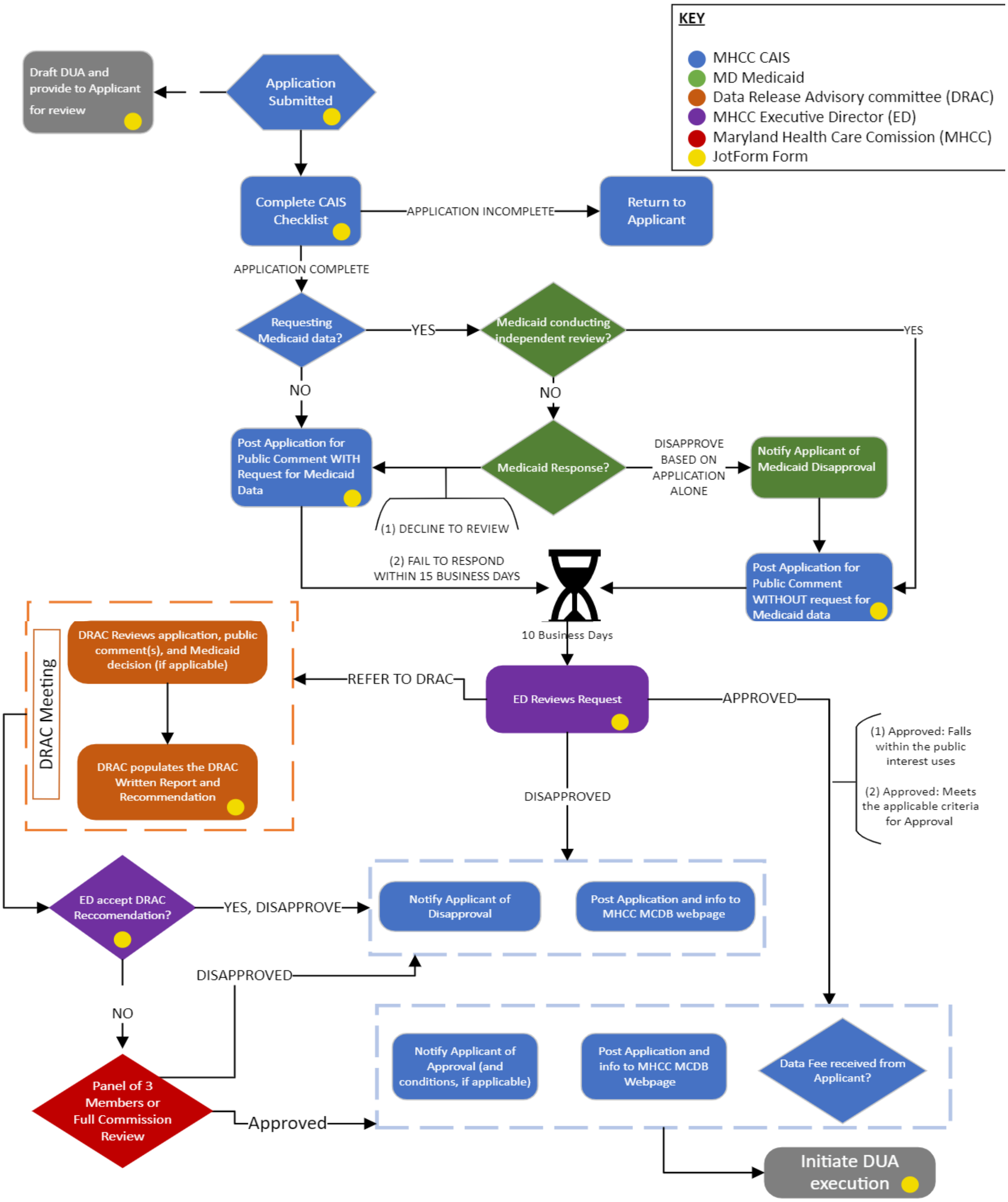
- Members of the DRAC shall serve for a term not to exceed 3 years. At the end of a term, a member continues to serve until a successor is appointed.
- A member of the DRAC may be reappointed.
- The Executive Director may remove a member of the DRAC for neglect of duty or misconduct by providing written notification to the DRAC member, stating the reason for the removal.
- A member of the DRAC who receives written notification of removal under §H of regulation may submit a written request for full Commission review of the Executive Director's removal decision within 20 business days of the date of the Executive Director's written notification of removal. The written request for full Commission review shall state with particularity the grounds and factual basis for the DRAC member's disagreement with the Executive Director's decision to remove the DRAC member.

Overview of Application Process

Application Review Process Diagram for Requests from Non-Government Agencies


KEY
● MHCC CAIS
● MD Medicaid
● Data Release Advisory Committee (DRAC)
● MHCC Executive Director (ED)
● Maryland Health Care Commission (MHCC)
● JotForm Form
Draft DUA and provide to Applicant for review
Application submitted
Complete CAIS Checklist
APPLICATION INCOMPLETE
Return to Applicant
APPLICATION COMPLETE
Requesting Medicaid data?
YES
Medicaid conducting independent review?
YES
NO
NO
Medicaid Response?
DISAPPROVE BASED ON APPLICATION ALONE
Notify Applicant of Medicaid Disapproval
(1) DECLINE TO REVIEW
(2) FAIL TO RESPOND WITHIN 15 BUSINESS DAYS
Post Application for Public Comment
Post Application for Public Comment WITHOUT request for Medicaid data
10 Business Days
DRAC Meeting
DRAC reviews application, public comment(s), and Medicaid decision (if applicable)
DRAC populates the DRAC Written Report and Recommendation
(1) APPROVE
(2) APPROVE WITH CONDITIONS
(3) DISAPPROVE
MHCC ED reviews DRAC Report & Recommendation and Public Comments
ED accept DRAC recommendation?
NO
Full Commission (or panel of 3 Commissioners) review & final decision
DISAPPROVE
YES, DISAPPROVE
Notify Applicant of Disapproval
Post Application and info to MHCC MCDB webpage
YES, APPROVE/ APPROVE WITH CONDITIONS
APPROVE/ APPROVE WITH CONDITIONS
Notify Applicant of Approval (and conditions, if applicable)
Post Application and info to MHCC MCDB webpage
Data fee received from Applicant?

Application Review Process Diagram for Requests from Government Agencies


KEY
● MHCC CAIS
● MD Medicaid
● Data Release Advisory committee (DRAC)
● MHCC Executive Director (ED)
● Maryland Health Care Comission (MHCC)
● JotForm Form
Draft DUA and provide to Applicant for review
Application Submitted
Complete CAIS Checklist
APPLICATION INCOMPLETE
Return to Applicant
APPLICATION COMPLETE
Requesting Medicaid data?
YES
Medicaid conducting independent review?
YES
NO
NO
Post Application for Public Comment WITH Request for Medicaid Data
Medicaid Response?
DISAPPROVE BASED ON APPLICATION ALONE
Notify Applicant of Medicaid Disapproval
(1) DECLINE TO REVIEW
(2) FAIL TO RESPOND WITHIN 15 BUSINESS DAYS
Post Application for Public Comment WITHOUT request for Medicaid data
10 Business Days
DRAC Meeting
DRAC Reviews application, public comment(s), and Medicaid decision (if applicable)
DRAC populates the DRAC Written Report and Recommendation
REFER TO DRAC
ED Reviews Request
APPROVED
(1) Approved: Falls within the public interest uses
(2) Approved: Meets the applicable criteria for Approval
DISAPPROVED
ED accept DRAC Reccomendation?
YES, DISAPPROVE
Notify Applicant of Disapproval
Post Application and info to MHCC MCDB webpage
DISAPPROVED
NO
Panel of 3 Members or Full Commission Review
Approved
Notify Applicant of Approval (and conditions, if applicable)
Post Application and info to MHCC MCDB Webpage
Data Fee received from Applicant?
Initiate DUA execution

Staff Review

Requests for Data from Nongovernmental Entities

Most of the requests for data that the DRAC will review will be requests for data from non-governmental entities. After a non-governmental applicant submits an application, staff will start the application review process for completeness upon receipt of the application and a nonrefundable application fee. Staff should review the application to ensure that the applicant has fully and completely responded to all questions on the application. In determining whether an application is complete, staff should consider whether the applicant has supplied sufficient information for a decision to be made on all of the review criteria.

COMAR 10.25.05.06A specifies information that the applicant must disclose as part of the application, including:

- All potential or approved funding sources.
- Any data sharing or other requirements imposed by a funding source as a condition of receipt of funding.
- Whether the applicant or any person or certain related entities has been the subject of or a party to an enforcement action involving unauthorized access, use, and disclosure of data including a data breach of HIPAA violation

The person who signs the application must affirm under penalties of perjury that all content in the application and any supplementary information are true to the best of their knowledge, information, and belief, as per COMAR 10.25.05.06A(5)(b).

If the application is not complete, staff should request additional information, documentation, answers to questions, and clarifications from the applicant and provide a reasonable deadline for the applicant to respond. The applicant should be instructed to supply a new affirmation with any supplementary information. If the applicant does not provide timely the requested information, staff should administratively close the application and notify the applicant that if the applicant would like to receive consideration on a data request, the applicant must submit a new application and application fee, as per COMAR 10.25.05.06B(7).

Requests for Data from Governmental Entities

Governmental entities may submit an abbreviated application. In addition, requests for data by governmental entities may undergo an expedited review directly by the Executive Director, rather than first being reviewed by the DRAC, as per COMAR 10.25.05.05C. “Governmental entities” is narrowly defined under the regulations to only include Maryland state entities and the federal government, as per COMAR 10.25.05.02B(17). Local municipalities or other state governments are treated like other non-governmental applicants. COMAR 10.25.05.05 details the requirements for governmental applicants.

Transparency of Data Request and Data Release Process

There are publication requirements both before and after a decision is made on a data release application. Nearly all completed applications must be posted to the Commission's website for the duration of the review process[1], as per COMAR 10.24.05.07A. After an application is published, there is a 10-business day comment period for members of the public. Any public comments received must be considered by the DRAC and the Executive Director as part of their review of the application.

Decisions on applications must also be published to MHCC's website, specifying whether the application was approved, approved with conditions, disapproved, or withdrawn, as per COMAR 10.24.05.07D. If an application has been approved, MHCC must also post the amount of fees charged for the requested data, a statement that all fees were waived, or in the case a partial wavier, the amount of fees waived. MHCC must also post a summary description of any product derived, in whole or part, from the data.

If an applicant has requested review of a decision by the full Commission pursuant to COMAR 10.24.05.11, MHCC must also note that further review is pending and post the final decision when the review process is completed.

[1] The only exception to this publication requirement are applications submitted by governmental entities pursuant to an express state or federal statutory or regulatory mandate.

DRAC Review

The DRAC's primary responsibility is to review a completed applications requests for data and make a written recommendation to the Executive Director. In addition, the DRAC may be called upon to provide advice, consultation, and expertise on issues and questions that may arise during staff's initial review of the application, during the Executive Director's review of the application, or after the data has been released, regarding compliance and enforcement of a data use agreement, as per COMAR 10.25.05.08.

Commission staff shall provide the necessary administrative support required for the DRAC to perform its duties and obligations, such as facilitating the scheduling and conducting of DRAC meetings, providing DRAC meeting agendas and supporting reference materials, conducting research and obtaining additional information as requested by the DRAC, and assisting in the preparation of written reports and recommendations.

DRAC Meeting Procedures

The DRAC will meet quarterly to review the pending applications. The meetings will be held virtually. The staff will send DRAC members the agenda, the meeting link, and any necessary documents three weeks prior to the meeting to allow for sufficient time for the members to review.

Voting will be limited to DRAC members in attendance at a convened meeting. A majority of DRAC members constitutes a quorum. All DRAC actions shall be by a majority of the quorum present and voting.

Three weeks prior to the quarterly meeting, DRAC members will receive via email and JotForm the application-related materials which will include the application itself; the data management plan; any public comments received; the Medicaid decision document, if applicable; any other related documents; the DRAC Review checklist.

A DRAC member must recuse themselves if the member has an "affiliation with an applicant, or with any entity sponsoring, participating, or otherwise affiliated with an applicant's proposed use of the requested data or any other conflict of interest or appearance of impropriety", as per COMAR 10.25.05.09E. Once recused, a member may not participate in any discussions with other DRAC members about the application or vote on the application.

Criteria for Approval and Disapproval

The regulations set specific criteria that the DRAC must consider when deciding whether to recommend approval of an application, along with any public comments received. COMAR 10.25.05.09. The Executive Director will review these same criteria when considering the DRAC's recommendation on the application.

In reviewing an application, the DRAC must consider each of the criteria for approval and disapproval and all public comments, as per COMAR 10.25.05.09B.

The review criteria require the DRAC to consider whether the scope of the request, the applicant's education and experience, and the applicant's data management plan demonstrate that the applicant will adequately safeguard the privacy and security of the data, and whether the proposed use of the data serves the public interest. In addition to considering the application's compliance with MHCC's regulations, the DRAC must consider whether the proposed use of the data complies with other State and federal laws relating to the privacy and securing of health information, including the Maryland Confidentiality of Medical Records Act, Md. Code Ann., Health-Gen. § 4-301 et seq, and the Health Insurance Portability and Accountability Act ("HIPAA") of 1996. A checklist with all review criteria is included at Appendix i.

Steps for the DRAC

The DRAC Needs More Information to Make a Recommendation (option)

The DRAC can ask MHCC staff to request additional information and documentation from the applicant,as per COMAR 10.25.05.09H. If the applicant fails to timely provide the information, the application will be administratively closed. The DRAC can also require the applicant to meet with the DRAC to provide additional information, answer questions, or provide clarification on the information provided in the application. Ideally the applicant will be available to answer questions when the DRAC meets to discuss an application.

The DRAC can also ask the Executive Director to invite an expert to assist the DRAC in the review of application. An individual invited to assist the DRAC must not have a conflict of interest and may not vote on the application.

Finally, the DRAC can require the applicant to obtain Institutional Review Board review prior to making a decision on the application.

Prepare Written Report and Recommendation

Once the DRAC is ready to make a recommendation on an application, it must submit a written report and recommendation on the application to the Executive Director, as per COMAR 10.25.05.09K. MHCC staff will assist with drafting a written report and recommendation for the DRAC's review. The report must address each of the review criteria for approval and disapproval, and any public comments received.

The DRAC may recommend either that the application be approved, be approved with conditions, or disapproved. A template for the Report and Recommendation is included at Appendix IV.

Post-DRAC Procedures

Decisions on Requests for Data

Most reviews of data request applications will end with the Executive Director. Applications that propose to develop and sell a product that contains de-identified data must be referred to the full Commission for a decision. Otherwise, other than applications by governmental entities that bypass the DRAC, the Executive Director will review and consider the DRAC's written report and recommendation in making a decision, as per COMAR 10.25.05.10. Like the DRAC, the Executive Director must review all public comments received and consider all the criteria for approval and disapproval. The Executive Director may send the application back to the DRAC for further review or consideration.

After reviewing all relevant information, the Executive Director will issue a written decision approving the application, approving the application subject to conditions, or disapproving the application. If the Executive Director's decision differs from the recommendation of the DRAC, the Executive Director's decision must be referred to the full Commission for final review.

Instead of making a decision, the Executive Director may also refer the application instead to a review panel of 3 Commission members, which shall include a consumer member of the Commission. The panel can either render a final decision on the application or refer it to the full Commission.

Review of Decisions

If an applicant is not satisfied with the decision of the Executive Director or review panel, as applicable, the applicant may submit a written request for full Commission review, as per COMAR 10.25.05.11. The applicant must submit this request within 20 business days of the date of the decision and must specifically address the grounds and factual basis for the applicant's disagreement with the decision. The applicant can request an opportunity to present oral argument. The full Commission shall issue a written decision affirming, reversing, or modifying the decision reviewed.

In those instances in which the application was sent to the full Commission for a decision, rather than to the Executive Director or review panel, the applicant can instead submit a request for reconsideration.

Data Use Agreement

Before any data can be released, the approved applicant must pay any fees and enter into a data use agreement (DUA) with MHCC. The regulations prescribe certain terms that must be included in the DUA, as per COMAR 10.25.05.13. If approval of any application is subject to any conditions, those conditions must be incorporated into the DUA. A template DUA is included at Appendix v.

There are a number of compliance and enforcement actions available to the Commission if a data recipient fails to comply with any of the terms of the DUA, or if it becomes subsequently known that the data recipient provided false information during the application process. COMAR 10.25.05.14.

JotForm Introduction

Thank you for serving as a member of the DRAC.

The MCDB data access application review process includes several stages of review, including sharing documents and obtaining formal signoff. We are using JotForm, an online tool, to automate the document flow process as much as possible. This document is a guide to accessing the MCDB/DRAC JotForm site, with instructions about how to provide your e-signature when needed.

Additionally, this document also includes diagrams showing DRAC decision points in the application process.

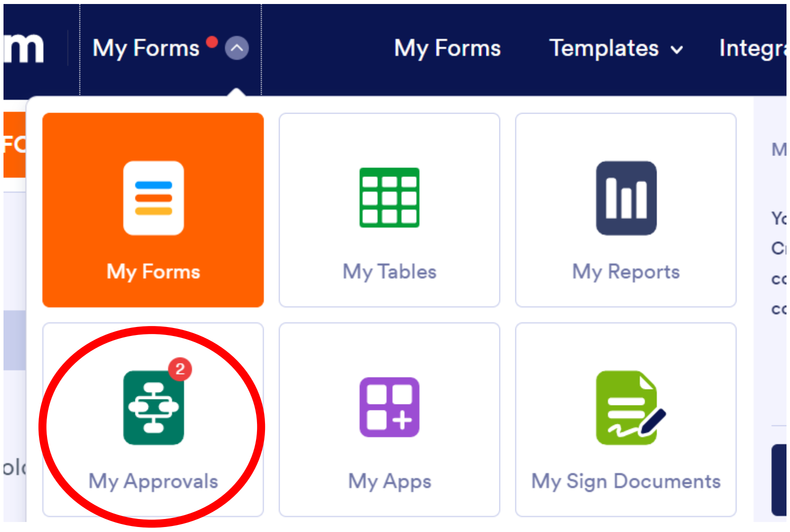
If you need help with accessing documents, providing signoffs or any other issue with JotForm, please reach out to CAIS Staff at mhcc.datarelease@maryland.gov. or contact Mahlet 'Mahi' Konjit-Solomon directly at Mahlet.Konjit-Solomon@maryland.gov

Getting Started

DRAC members review the DRAC Report and Recommendation form for a given application through an email from jotform, DRAC members will select the option aligned with the DRAC decision. The options are "approval", "disapproval" and if the DRAC member have not attended the meeting or had to recuse themselves then "did not attend" can be selected.

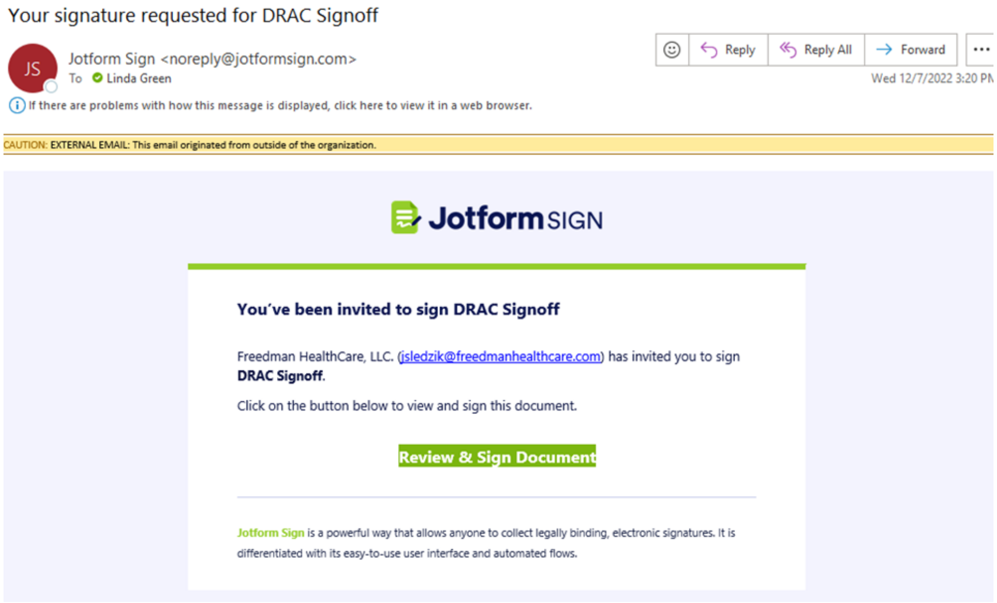
If you choose to create an account, please do so with the email address you have provided to MHCC. This will ensure that the document will come to your inbox in JotForm.

Once in JotForm, you can find your action items by clicking on "My Approvals".



Review and Notification Screens

CAIS staff will complete the DRAC Report and Recommendation during the DRAC meeting and send it to the DRAC Chair for approval. After the Chair approval, the report will be sent sequentially to each DRAC member, alphabetically by last name. When a Report and Recommendation form is ready for viewing, a link will be sent to your email address from noreply@jotformsign.com. Clicking on the link in the email notifications will take you to the action step. Each DRAC member's review will send the report to the next member. Below is the email notification you will receive when it is your turn to review the report. Click on the Review & Sign Document to open the report.



Your signature requested for DRAC Signoff

Jotform Sign <noreply@jotformsign.com>
To Linda Green

Wed 12/7/2022 3:20 PN

If there are problems with how this message is displayed, click here to view it in a web browser.

CAUTION: EXTERNAL EMAIL: This email originated from outside of the organization.

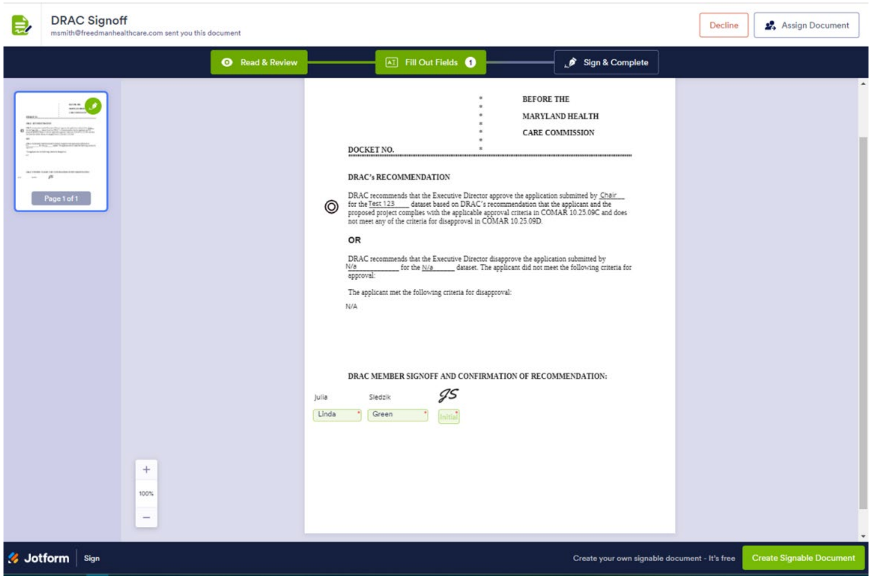
You've been invited to sign DRAC Signoff

Freedman HealthCare, LLC. (jsledzik@freedmanhealthcare.com) has invited you to sign **DRAC Signoff**.

Click on the button below to view and sign this document.

Jotform Sign is a powerful way that allows anyone to collect legally binding, electronic signatures. It is differentiated with its easy-to-use user interface and automated flows.

Once open, the report will look like the image below.



DRAC Signoff
msmith@freedmanhealthcare.com sent you this document

BEFORE THE
MARYLAND HEALTH
CARE COMMISSION

DOCKET NO.

DRAC's RECOMMENDATION

DRAC recommends that the Executive Director approve the application submitted by Chair for the Test 123 dataset based on DRAC's recommendation that the applicant and the proposed project complies with the applicable approval criteria in COMAR 10.25.09C and does not meet any of the criteria for disapproval in COMAR 10.25.09D.

OR

DRAC recommends that the Executive Director disapprove the application submitted by N/a for the N/a dataset. The applicant did not meet the following criteria for approval:

The applicant met the following criteria for disapproval:

N/A

DRAC MEMBER SIGNOFF AND CONFIRMATION OF RECOMMENDATION:

Julia Sledzik JS

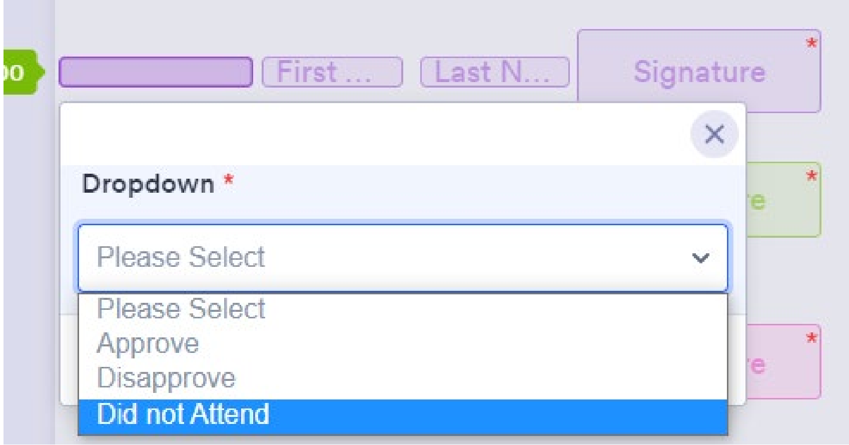
Linda Green Initial

Please review the report that has been filled out by the CAIS Staff. When you have completed your review, on the drop-down menu located to the left of the name and signature boxes, you may choose “Approve”, “Disapprove”, or “Did not attend”.

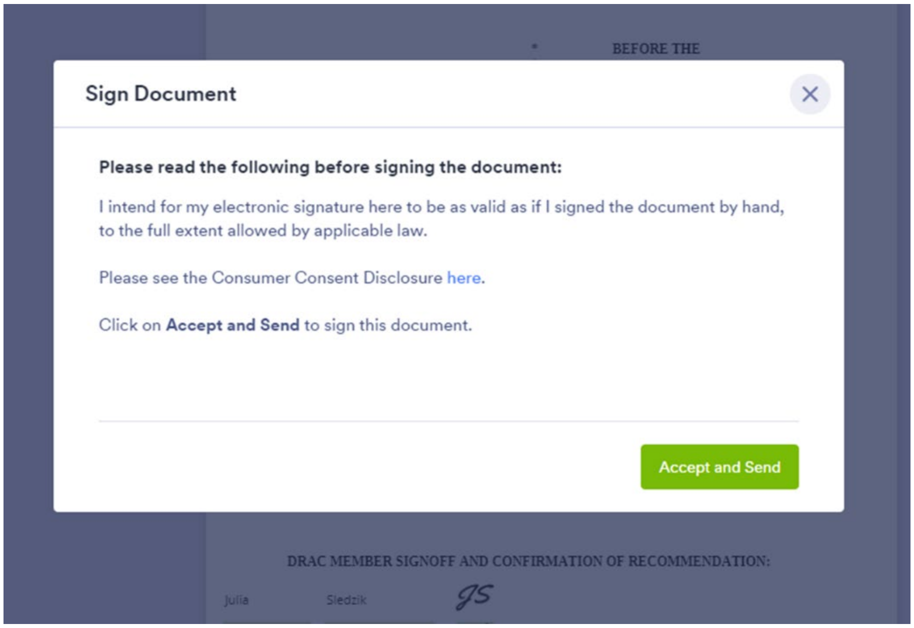
Approve: Agree that the report shows what was discussed at the meeting.

Disapprove: The report does not show what was discussed at the meeting. Please reach out to the DRAC Chair and CAIS Staff for next steps.

Did not attend: If you did not attend the Committee meeting, choose “Did not attend.”



Please remember the report will not move to the next DRAC member until you accept and complete. To accept, click “Accept and Send”.



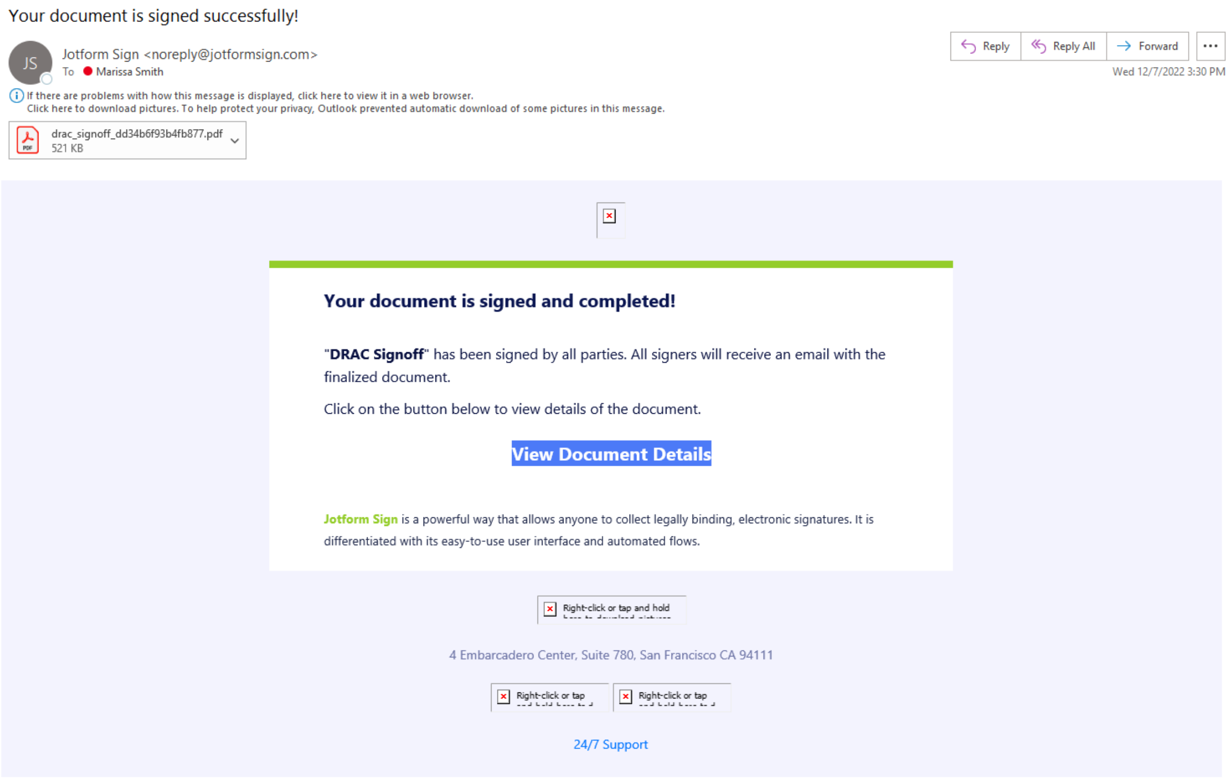
Please read the following before signing the document:

I intend for my electronic signature here to be as valid as if I signed the document by hand, to the full extent allowed by applicable law.

Please see the Consumer Consent Disclosure here.

Click on **Accept and Send** to sign this document.

After clicking “Accept and sign,” you will receive a confirmation email and the document will move to the next committee member.



Your document is signed successfully!

Jotform Sign <noreply@jotformsign.com>
To Marissa Smith

Wed 12/7/2022 3:30 PM

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

drac_signoff_dd34b6f93b4fb877.pdf
521 KB

Your document is signed and completed!

"**DRAC Signoff**" has been signed by all parties. All signers will receive an email with the finalized document.

Click on the button below to view details of the document.

View Document Details

Jotform Sign is a powerful way that allows anyone to collect legally binding, electronic signatures. It is differentiated with its easy-to-use user interface and automated flows.

4 Embarcadero Center, Suite 780, San Francisco CA 94111

24/7 Support

After all members have signed, each member will receive the signed document from JotForm in an email.

If you need help at any point, please reach out to CAIS Staff at mhcc.datarelease@maryland.gov. Thank you!

Appendix

i. DRAC Criteria Checklist
ii. CAIS Criteria checklist
iii. ED Checklist and Review
iv. Report and Recommendation Template
v. Template DUA
vi. COMAR 10.25.05
vii. DRAC Review Checklist

MARYLAND
Health Care
Commission

MD APCD DATA RELEASE ADVISORY COMMITTEE (DRAC)
REVIEW REQUIREMENTS GUIDE

DRAC Responsibilities for Application Review		
1	Criteria for Approval	COMAR 10.25.05.09C
2	Criteria for Disapproval	COMAR 10.25.05.09D
3	Recusal	COMAR 10.25.05.09E
4	External Opinion	COMAR 10.25.05.09F
5	IRB Review	COMAR 10.25.05.09G
6	Request for additional information	COMAR 10.25.05.09H
7	Request for meeting	COMAR 10.25.05.09I
8	Public Comment Reviewed	COMAR 10.25.05.09J

ID #	CRITERIA FOR APPROVAL (COMAR 10.25.05.09C)	Met? (Y/N)
1	Has the applicant provided documentation of relevant education, training, and experience that demonstrates the applicant is capable of undertaking and accomplishing the objective of the proposed use of the data and being a responsible steward of the requested data?	
2	Are the data elements requested by an applicant the minimum amount necessary to achieve the intended purpose for which the data is requested?	
3	Does the proposed use of the data comply with applicable State and federal laws, including those laws relating to the privacy and security of protected health information?	
4	Has the applicant provided a written data management plan that demonstrates appropriate privacy and security controls for access and storage of the data and for safeguarding individual privacy and preventing unauthorized access and use of the data?	
5	Can the requirement of obtaining written authorization from each individual who is the subject of requested identifiable data be waived in accordance with 45 CFR § 164.512?	
6	If the applicant has proposed linkage of the requested data to other data source(s), has the applicant has provided:	
6a	Sufficient written justification of the need to link the requested data to the other data source(s) named in the application to accomplish the objective and achieve the results of the proposed use of the data; and	
6b	Written proof that an additional level of data privacy and security controls will be in place to protect the privacy and identification of the individuals who are the subject of the requested data and the other data source(s) to which the requested data is to be linked.	
7	If an applicant proposes to develop and sell a product that contains de-identified data, has the applicant provided satisfactory written justification of how the proposed sale of the product using the de-identified data will serve the public interest?	
8	Is the proposed use of the data in the public interest?	

ID #	CRITERIA FOR DISAPPROVAL (COMAR 10.25.05.09D)	Does the Application demonstrate any of the following criteria for disapproval? (Y/N)
1	The proposed use of the data violates State or federal law.	
2	The proposed use of the data is not in the public interest.	
3	The proposed use of the data is designed so that the stated objective of the project cannot be met.	
4	False information or documentation on, or related to, the application was provided to Commission staff, the DRAC, the Executive Director, or the Commission.	
5	The applicant provided incomplete information upon which to base a decision on the application.	
6	The applicant or any person or entity that is an officer, owner, operator, or part of management of an applicant's organization who will have access and use of the requested data is not currently, or has not been within ten (10) years prior to the date of the application, a subject of, or a party to a state or federal regulatory agency action or civil or criminal action involving a data breach, HIPAA violation or other matter involving unauthorized access, use, and disclosure of data regardless of whether there has been a finding or admission of guilt, including being:	
6a	Convicted of a felony or pleading guilty, nolo contendere, entering a best interest plea of guilty, or receiving a diversionary disposition regarding a felony;	
6b	A subject of an investigation conducted by, or a pending complaint, charges, or indictment issued by a local, state, or federal governmental regulatory agency or other state or federal law enforcement agency; or	
6c	A party to a final dispositive action in a state or federal governmental agency regulatory action or a civil action that resulted in entry into a settlement agreement, consent agreement, decree, or order, a corporate integrity agreement, corrective action agreement, or other similar agreement or other disposition in a civil action regardless of whether there has been an admission or finding of guilt or liability.	
7	The applicant violated a previous data use agreement.	
8	The data management plan does not demonstrate privacy and security controls for safeguarding individual privacy and preventing unauthorized access to or use of the data.	
9	The proposed use of the data is for an impermissible purpose.	
10	The applicant who proposes to develop and sell a product that contains requested de-identified data has not provided satisfactory written justification of how the proposed sale of the product using the de-identified data will serve the public interest.	

MARYLAND
Health Care
Commission

Center for Analysis and Information Systems
Data Release Application Review

Application Number	
Project Title:	
MHCC Approved Pre-Application Number	
Requesting Organization	
Date Pre-Application Submitted	
Date Submitted:	
Date Reviewed by CAIS:	12-08-2022
Date DRAC Meeting to Consider this Application	

1. Preliminary Review

a. Pre-Application Approved by CAIS?

□Yes □No

b. Application fee received?

□Yes □No

c. Does this request include Medicaid data?

If so:

i.	Date sent to Medicaid:	
ii.	Medicaid review period end date:	
iii.	Date response received from Medicaid:	

2. Project Information

		Yes	No
a.	Research questions or intended product is permitted. *Comment*:		
b.	Purposes reflect public health importance. *Comment*:		
c.	Proposed use is in the public interest. *Comment*:		

		Yes	No
d.	Project methodology clearly describes analytic processes *Comment*:		
e.	IRB Review provided *Comment*:		
3.	**Publication and Dissemination**		
a.	Is the plan for publication permitted under COMAR? *Comment*:		
b.	Is the dissemination method described? *Comment*:		
c.	Is cell size suppression fully described? *Comment*:		
d.	Are the geographic units appropriate? *Comment*:		
e.	Will the results be used for consulting purposes? *Comment*:		
f.	Will the results be included in products for sale? *Comment*:		
g.	Will results be used to develop a software product or in a tool? *Comment*:		
h.	Will the results be used in some other way? *Comment*:		
i.	Will the results be privately disseminated? *Comment*:		
j.	Will the data be used for price transparence purposes? *Comment*:		
k.	Will providers be identified? If so, is the provider review process adequately described? *Comment*:		
4.	**Data Specifications**		
a.	Are the justifications for the requested files consistent with the project as described? *Comment*:		
5.	**Additional Data Sources**		
i.	Medicare data: Is the applicant under contract to a Maryland state agency? *Comment*:		
ii.	Medicaid data: Did the Applicant provide a Medicaid approval letter? *Comment*:		
6.	**Linkages**		
a.	Are the linkages clearly described and feasible? *Comment*:		
b.	Does the justification support the request? *Comment*:		

		Yes	No
c.	Could the research goal be accomplished without the linked data? *Comment*:		
d.	Does the plan for preventing re-identification provide appropriate protections? *Comment*:		
7.	**Data Management Plan**		
a.	Is the plan for physical possession and storage of the data appropriate, adequate and consistent with best practices? *Comment*:		
b.	Is the physical and technical infrastructure appropriate for the requested data? *Comment*:		
c.	Are the controls on data sharing, transmission and distribution effective and consistent with best practices? *Comment*:		
d.	Are the policies and procedures for data destruction consistent with the proposed data storage and access methods? *Comment*:		

Upon review of this application, the CAIS staff recommend the following action:

□ **Forward to Executive Director with recommendation to approve**
□ **Forward to Executive Director with recommendation to disapprove**
□ **Forward to DRAC for consideration**

Date:

CAIS Staff:

MARYLAND
Health Care
Commission

Executive Director Data Request Application Decision

Application Review Checklist:

- ❑ Application with preliminary Data Use Agreement
- ❑ CAIS application recommendation
- ❑ Medicare Data Use Request (If applicable)
- ❑ Medicaid review and decision (If applicable)
- ❑ Public Comments
- ❑ Data Release Advisory Committee's written report and recommendation
- ❑ CAIS staff final recommendation

Application ID:

Applicant Type: □ Governmental Entity □ Non-Governmental Entity

For governmental entity applicants:

➢ Does the proposed use of the data requested fall within the public interest uses described in Regulation .01B of 10.25.05 (10.25.05.05.E(1))?

□ Yes □ No

For governmental AND non-governmental entity applicants:

➢ Approval criteria set forth in 10.25.05.09C met?

□ Yes □ No

➢ Any of the disapproval criteria set forth in 10.25.05.09C exist for disapproval of this application under 10.25.05.09D?

□ Yes □ No

➢ Does the application include a proposal to develop and sell a product that contains requested de-identified data (10.25.05.10.F)?

□ Yes □ No

If **YES**, the Executive Director **MAY NOT** make a decision on the application and shall refer the application, the DRAC's written report and recommendation, and all public comments received on the application to the full Commission for a decision.

If **NO**, please continue to next page (page 2).

After careful review of all application materials and supplements, public comments, the Data Release Review Committee's recommendation, and the CAIS staff final recommendation, I have decided to:

- ❑ Fully approve the applicant's request for MCDB data.
- ❑ Partially approve the applicant's request for MCDB data with the conditions detailed below.
- ❑ Disapprove the applicant's request for MCDB data.
- ❑ Refer application back to the DRAC with a request that the DRAC, through Commission staff, obtain and provide more specific or additional information, conduct a more detailed review and evaluation of the review criteria (10.25.05.10.B)
- ❑ Refer the DRAC's written report and recommendation, and all public comments received, to a review panel of 3 Commission members, which shall include a consumer member of the Commission (10.25.05.10.E)

Conditions for approval:

Print Name

Sign Name

Date

Date written decision notifying the applicant of the decision and any reasons for disapproval, if applicable, sent:

Does the Executive Director's decision align with the DRAC recommendation (10.25.05.10D)?

☐ Yes ☐ No

If **YES**, did the Executive Director's decide to approve an application that the DRAC recommended be disapproved, or to disapprove an application that the DRAC recommended be approved?

☐ Yes ☐ No

If **YES**, the Executive Director shall prepare a proposed recommended decision and refer to the full Commission for consideration and issuance of a final decision affirming, reversing, or modifying the Executive Director's recommended decision.

	*	**BEFORE THE**
	*	
	*	**MARYLAND HEALTH**
	*	
	*	**CARE COMMISSION**
	*	
DOCKET NO.	*	

****

DRAC Report and Recommendation

TABLE OF CONTENTS

I. APPLICATION

a. The Applicant

b. The Project

i. **Project Purpose**

ii. **Project Data Sources**

iii. **Project Funding Source**

iv. **Proposed Project Methodology**

v. **Data Requested**

vi. **Project Timeline**

vii. **Project Outcome**

viii. **Data Fees**

c. The Team

II. DRAC'S REVIEW

a. COMAR 10.25.09C- Criteria for Approval

i. **COMAR 10.25.09C(1) An applicant has provided documentation of relevant education, training, and experience that demonstrates the applicant is capable of undertaking and accomplishing the objective of the proposed use of the data and being a responsible steward of the requested data.**

The applicant has provided documentation of_________

The applicant ☐ is [☐ is not] capable of undertaking and accomplishing its objectives because

DRAC concludes the applicant ☐ has [☐ has not] met this criterion.

ii. **COMAR 10.25.09C(2) The data elements requested by an applicant are the minimum amount necessary to achieve the intended purpose for which the data is requested.**

The applicant is requesting

This ☐ is [☐ is not] the minimum amount necessary for the applicant to

because

DRAC concludes the applicant ☐ has [☐ has not] met this criterion.

iii. **COMAR 10.25.09C(3) The proposed use of the data complies with applicable State and federal laws, including those laws relating to the privacy and security of protected health information (PHI).**

Either:
☐ The applicant's proposed use of the data complies with all applicable State and federal laws.
or
☐ The proposed use does not comply, if so, specify why it does not comply.

DRAC concludes the applicant ☐ has [☐ has not] met this criterion.

iv. **COMAR 10.25.09C(4) The applicant has provided a written data management plan that demonstrates appropriate privacy and security controls for access and storage of the data and for safeguarding individual privacy and preventing unauthorized access and use of the data.**

DRAC has reviewed the applicant's data management plan. The plan demonstrates [☐ does not demonstrate] appropriate privacy and security controls because

DRAC concludes the applicant ☐ has [☐ has not] met this criterion.

v. **COMAR 10.25.09C(5) The requirement of obtaining written authorization from each individual who is the subject of requested identifiable data can be waived in accordance with 45 CFR §164.512.**

DRAC finds that the use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals. As stated in §II(a)(iv), the applicant has submitted a data management plan that demonstrates appropriate privacy and security control that would protect the identifiers from improper use and disclosure. In addition, the applicant's data management plan includes an adequate plan to destroy the data at the earliest opportunity. The applicant has agreed that the protected health information will not be reused or disclosed to any other person or entity.

DRAC further finds that the research could not be practicably conducted without the waiver and without access and use of the protected health information because

DRAC concludes the applicant ☐ has [has not] met this criterion.

vi. **COMAR 09.C (6) If the applicant has proposed linkage of the requested data to other data source(s), the applicant has provided:**

a. **COMAR 10.25.09C(6)(a) Sufficient written justification of the need to link the requested data to the other data source(s) named in the application to accomplish the objective and achieve the results of the proposed use of the data; and**

The applicant proposes to link the MCDB data with

The applicant states that it needs to link the data because

DRAC finds that this ☐ is [☐ is not] an appropriate justification because

DRAC concludes the applicant ☐ has [☐ has not] met this criterion.

or

☐ The applicant has not proposed to link the requested data to any other data sources. Therefore, this criterion does not apply.

b. **COMAR 10.25.09C(6)(b) Written proof that an additional level of data privacy and security controls will be in place to protect the privacy and identification of the individuals who are the subject of the requested data and the other data source(s) to which the requested data is to be linked.**

The applicant's data management plan proposes to provide an additional level of data privacy and security controls by

This ☐ is [☐ is not] sufficient to protect the privacy and identification of individuals who are the subject of the data because

DRAC concludes the applicant ☐ has [☐ has not] met this criterion.

vii. **COMAR 10.25.09C(7) An applicant who proposes to develop and sell a product that contains de-identified data has provided satisfactory written justification of how the proposed sale of the product using the de-identified data will serve the public interest.**

The applicant proposes to

The proposed product ☐ is [☐ is not] in the public interest because

DRAC concludes the applicant ☐ has [☐ has not] met this criterion.

or

☐ The applicant does not propose to develop or sell a product. This criterion does not apply.

viii. **COMAR 10.25.09C(8) The proposed use of the data is in the public interest. Examples of uses of data that serve the public interest include:**

a. **COMAR 09.C (8)(a) Health care cost and utilization analysis to guide and develop public policy;**

b. **COMAR 09.C (8)(b) Studies that promote improvement in public health, health care quality, and health care access;**

c. **COMAR 09.C (8)(c) Health planning and resource allocation studies;**

d. **COMAR 09.C (8)(d) Making information on cost and quality accessible to the public; and**
e. **COMAR 09.C (8)(e) Studies directly tied to evaluation and improvement of federal and State government initiatives.**

The applicant proposes to use the data to

This ☐ is [☐ is not] in the public interest because

DRAC concludes the applicant ☐ has [☐ has not] met this criterion.

b. COMAR 10.25.09D Criteria for Disapproval

i. **COMAR 10.25.09D(1) The proposed use of the data violates State or federal law.**

As stated in §II(a)(iii), the applicant's proposed use ☐ does [☐ does not] violate State or federal law.

DRAC concludes that the applicant ☐ has [☐ has not] met this criterion for disapproval.

ii. COMAR 10.25.09D(2) The proposed use of the data is not in the public interest.

As described in §II(a)(vii), the applicant's proposed use of the data ☐ is [☐ is not] in the public interest.

DRAC concludes that the applicant ☐ has [☐ has not] met this criterion for disapproval.

iii. **COMAR 10.25.09D(3) The proposed use of the data is designed so that the stated objective of the project cannot be met.**

The applicant proposes to use the data to

in order to

DRAC does not know whether the applicant:

☐ *will be able to achieve its objective but believes that it has developed an appropriate plan to enable it to do so.*

or

☐ *The applicant will not be able to achieve its objective because*

DRAC concludes that the applicant ☐ has [☐ has not] met this criterion for disapproval.

iv. **COMAR 10.25.09D(4) False information or documentation on, or related to, an application was provided to Commission staff, the DRAC, the Executive Director, or the Commission**

The applicant ☐ has [☐ has not] provided any false information or documentation to the Commission staff or DRAC.

DRAC concludes that the applicant ☐ has [☐ has not] met this criterion for disapproval.

v. **COMAR 10.25.09D(5) An applicant provided incomplete information upon which to base a decision on the application.**

☐ The applicant has provided complete information.

or

☐ The applicant has failed to provide complete information about

DRAC concludes that the applicant ☐ has [☐ has not] met this criterion for disapproval.

vi. **COMAR 10.25.09D(6) An applicant or any person or entity that is an officer, owner, operator, or part of management of an applicant's organization who will have access and use of the requested data is currently, or has been within 10 years prior to the date of the application, a subject of or a party to a state or federal regulatory agency action or civil or criminal action involving a data breach, HIPAA violation, or other matter involving unauthorized access, use, and disclosure of data regardless of whether there has been a finding or admission of guilt, including being:**

a. **(a) Convicted of a felony or pleading guilty, nolo contendere, entering a best interest plea of guilty, or receiving a diversionary disposition regarding a felony;**

b. **(b) A subject of an investigation conducted by, or a pending complaint, charges, or indictment issued by a local, state, or federal governmental regulatory agency or other state or federal law enforcement agency; or**

c. **(c) A party to a final dispositive action in a state or federal governmental agency regulatory action or a civil action that resulted in entry into a settlement agreement, consent agreement, decree or order, corporate integrity agreement, corrective action agreement, or other similar agreement or other disposition in a civil action regardless of whether there has been an admission or finding of guilt or liability.**

Neither the applicant or any person or entity that is an officer, owner, operator of the applicant's organization who will have access and use of the requested data is currently or has been within the last 10 years subject of or a party to a state or federal regulatory agency action or civil or criminal action involving a data breach, HIPAA violation, or other matter involving unauthorized access, use, and disclosure of data regardless of whether there has been a finding or admission of guilt.

DRAC concludes that the applicant □ has [□ has not] met this criterion for disapproval.

vii. **COMAR 10.25.09D(7) Violation of a previous data use agreement.**

□ The applicant has not violated a previous data use agreement.
or
□ The applicant previously entered into a data use agreement with the Commission on
The applicant violated that data use agreement by

DRAC concludes that the applicant □ has [□ has not] met this criterion for disapproval.

viii. **COMAR 10.25.09D(8) The data management plan does not demonstrate privacy and security controls for safeguarding individual privacy and preventing unauthorized access to or use of the data.**

As described in §II(a)(iv), the applicant's data management plan ☐ demonstrates [☐ does not demonstrate] appropriate privacy and security controls. DRAC concludes that the applicant

☐ has [☐ has not] met this criterion for disapproval.

ix. **COMAR 10.25.09D(9) The proposed use of the data is for an impermissible purpose, which includes but is not limited to:**
    a. **(a) Using the requested data to identify an individual using a particular product or drug in order to develop a marketing campaign and directly contact an individual;**

    b. **(b) Using the requested data to contact an individual for fund-raising purposes directly; and**

    c. **(c) Using the requested data to contact an individual who is the subject of the data for any reason.**

The applicant proposes to use the data to

This ☐ is [☐ is not] an impermissible purpose.

DRAC concludes that the applicant ☐ has [☐ has not] met this criterion for disapproval.

x. **COMAR 10.25.09D(10) An applicant who proposes to develop and sell a product that contains requested de-identified data has not provided satisfactory written justification of how the proposed sale of the product using the de-identified data will serve the public interest.**

As described in §(a)(vii), the applicant's produce will serve the public interest.

DRAC concludes that the applicant ☐ has [☐has not] met this criterion for disapproval.

or

☐ The applicant does not propose to develop or sell a product. This criterion does not apply.

c. Public Comments

Public comments were received from:

☐ No public comments were received with respect to this application.

III. DRAC'S RECOMMENDATION

☐ DRAC recommends that the Executive Director approve the application submitted by

for the
dataset based on DRAC's recommendation that the applicant and the proposed project complies with the applicable approval criteria in COMAR 10.25.09C and does not meet any of the criteria for disapproval in COMAR 10.25.09D.

OR

☐ DRAC recommends that the Executive Director disapprove the application submitted by
for the
dataset.

The applicant did not meet the following criteria for approval:

The applicant met the following criteria for disapproval:

DATA USE AGREEMENT BETWEEN THE

MARYLAND HEALTH CARE COMMISSION AND

This Data Use Agreement (“Agreement”) is made by and between the Maryland Health Care Commission (“MHCC” or “the Commission”), located at 4160 Patterson Avenue, Baltimore, Maryland 21215, and ______ (the “Data Recipient”) located at

____

(each a “Party” and, collectively, the “Parties”), to govern the release, use, privacy and security of Maryland Medical Care Data Base (“MCDB”) data provided by MHCC to the Data Recipient.

WHEREAS, under §§19-103(c)(3) and (4) and 19-133 of the Health-General Article of the Annotated Code of Maryland, and COMAR 10.25.06, MHCC is authorized to collect and store, *inter alia*, health care claims data for Maryland residents enrolled in commercial insurance, Medicare and the Medicaid Assistance Program (“Medicaid”) managed care organizations, and non- Maryland residents enrolled in Maryland commercial insurance plans, in the Maryland Medical Care Data Base (“MCDB”);

WHEREAS, the Data Recipient, by written application dated _______________ submitted to MHCC, requested access to the following data sets:

MCDB commercial claims data files for calendar years__________ Medicaid data claims files for calendar years ____
for a project entitled, ____________________________________

WHEREAS, the MCDB data is patient-specific data containing both protected health information (“PHI”) and personally identifiable information (“PII”), including unique patient identification numbers (encrypted), partial dates of birth, sex of patient, zip code of residence, provider identification numbers, diagnosis codes, dates of service, and insurer plan and type of product information; thus, MHCC and the Data Recipient consider the security and confidentiality of this data to be a matter of high priority.

NOW THEREFORE, in consideration of the mutual promises and covenants, the sufficiency of which is hereby acknowledged, MHCC and the Data Recipient agree as follows:

AGREEMENT

The above recitals and following attachments are fully incorporated into this Agreement:

Attachment A – Covered Data;
Attachment B – Scope of Work and Project Methodology
Attachment C – Additional Data Sources
Attachment D – Data Users Log;
Attachment E – Data Management Plan and Data Storage Location; and
Attachment F – Certificate of Data Destruction.

If the Data Recipient is receiving Medicare data, the following Addendum shall be incorporated into this Agreement:

Addendum 1: Medicare Data Use by Maryland State Agencies and their Contractors

If the Data Recipient is receiving Medicaid data, the following Addendum shall be incorporated into this Agreement:

Addendum 2: Medicaid Data Use Requirements

1. DATA TO BE RELEASED

1.1 MHCC will provide to Data Recipient the electronic files described in Attachment A ("Covered Data").

1.2 The Covered Data files will have a "SAS7BDAT" extension. MHCC will send the Covered Data to Data Recipient via a SSH File Transport Protocol (SFTP). Data Recipient agrees to set up an appropriate location to download the covered data in compliance with this Agreement and the Data Management Plan contained in Attachment E ("Data Management Plan and Data Storage Location").

1.3 Data Recipient agrees that MHCC shall retain all ownership rights to the Covered Data provided to Data Recipient and that Data Recipient does not obtain any right, title, or interest in any of the data provided by MHCC.

2. PERMITTED USES OF THE COVERED DATA

2.1 The Covered Data shall be used solely to support the project entitled

____

as described in Attachment B ("Scope of Work"), and other future projects to be reviewed and approved by MHCC. Any other uses of the Covered Data outside of the Scope of Work described in Attachment B are strictly prohibited unless prior written approval is obtained from MHCC.

2.1.1 Data Recipient in its application states a plan to use the Covered Data as follows: s:

2.1.2. Projects that include dissemination of the data through published studies or other public release must be submitted to MHCC for review prior to publication on its website. Other conditions include:

2.2 Data Recipient may retain the Covered Data and utilize such data for the specific purposes described in Attachment B during the effective dates of this Agreement.

2.3 Data Recipient agrees to provide a list of any files from sources other than the Covered Data that it plans to use in conjunction with the Covered Data in its analysis. Attachment C ("Additional Data Sources") contains all additional data sources known to Data Recipient at the time of execution of this Agreement. Data Recipient shall update this list, and provide such update to MHCC, prior to the use of any new data source(s) in conjunction with the Covered Data. Data Recipient further agrees not to link member-level data to any additional data source.

2.4 Data Recipient agrees that any use of the Covered Data in the creation of any document (report, study, manuscript, table, chart, etc.) must adhere to MHCC's cell size suppression policy unless MHCC approves the use of an alternate cell size. This policy requires that no cell of ten (10) or less may be displayed and that no use of percentages or other mathematical formulas may be used if they are based on a sample of ten (10) or fewer patients.

2.5 Data Recipient agrees not to disclose direct findings, listings, or information derived from the Covered Data, with or without direct identifiers, if such findings, listings, or information can, by themselves or in combination with other data, be used to deduce an individual's identity. Examples of such data elements include, geographic location, age (if > 89), sex, diagnosis and procedure, admission/discharge date(s), or date of death.

2.6 Data Recipient agrees not to attempt to re-identify individuals whose information is contained in the Covered Data. Data Recipient further agrees to not attempt to link any Covered Data to any other source of clinical or health service information.

3. PERMITTED USERS OF THE COVERED DATA

3.1 Data Recipient shall limit access to the Covered Data, the Covered Data documentation, and any files derived from the Covered Data to the minimum number of individuals necessary, as determined within the sole discretion of Data Recipient, to achieve the purposes set out in Attachment B, and access to the data shall be granted with minimal access and risk to Protected Health Information (PHI), in accordance with the Health Insurance Portability and Accountability Act ("HIPAA") of 1996, and the implementing regulations at 45 CFR Parts 160 and 164, specifically, 42 CFR § 164.512.

3.2 Data Recipient shall keep a log of the identity of each individual ("Data User") who is authorized to access the Covered Data. Attachment D ("Data Users Log") contains the log of authorized Data Users known to Data Recipient at the time of execution of this Agreement. After execution of this Agreement, Data Recipient will provide updates of the log to MHCC before authorizing any new individual to access the Covered Data.

3.3 Data Recipient shall be responsible for making all individuals who are permitted Data Users of the Covered Data under this Agreement, including any personnel of contractors and subcontractors, aware of the terms and conditions of this Agreement. Specifically, Data Recipient shall advise all Data Users of the confidential nature of the Covered Data and the safeguards required to protect the security of the data. In addition, Data Recipient shall provide a copy of this Agreement to all Data Users, inform them that they are required to comply with all terms and conditions of this Agreement, and obtain written acknowledgments from each Data User. Data Recipient shall provide documentation of Data Users' written acknowledgments to MHCC upon request.

4. DATA SECURITY and CONFIDENTIALITY

4.1 Data Recipient agrees to comply with any applicable State and federal confidentiality and security requirements regarding collection, maintenance, and use of the Covered Data, including HIPAA and the implementing regulations at 45 CFR Parts 160 and 164, and the Maryland Confidentiality of Medical Records Act ("MCMRA"), Md. Code Ann., Health-Gen §§ 4-301 *et seq*.

4.2 The Covered Data is confidential and shall not be disclosed or transferred without written consent of MHCC to anyone or entity other than the authorized Data Users listed in Attachment D ("Data Users Log").

4.3 Data Recipient will maintain the electronic security of the Covered Data in accordance with the Data Management Plan ("DMP") submitted by Data Recipient (Attachment E) for each data custodian. Each DMP, which shall be consistent with the State of Maryland Information Security Policy, and relevant State and federal laws, must be approved by MHCC prior to the release of data to Data Recipient.

4.3.1 The Covered Data shall be stored and processed so as to protect the confidentiality of the data, and in such a way that unauthorized persons cannot retrieve such records by means of computer, remote terminal, or any other means. If the Covered Data is stored in a folder on a network drive, that folder shall be omitted from the standard data back-up process utilized by Data Recipient. If the Covered Data is stored on a local hard drive, that computer must be in a secure location at all times.

4.3.2 Data Recipient will submit a revised DMP (Attachment E) to MHCC if there are any changes to the plan, including, but not limited to, storage location (in which case a revised Data Storage Location form) must also be submitted) and security protocols. MHCC must review and approve any revised DMP (and Data Storage Location, if applicable) before such plan is implemented.

4.4 At the termination of this Agreement for any reason, Data Recipient agrees to destroy the Covered Data, any products created from the Covered Data, and all back-up and archived copies of the Covered Data. The destruction process shall ensure that the data is erased from all networks, drives or computers and could involve using software such as WipeDrive that is capable of destroying data on a drive in a manner that meets the data destruction standards specified by the National Institute of Standards and Technology("NIST") Special Publication 800-88, Guidelines for Media Sanitation. Data Recipient will send a fully executed Certificate of Data Destruction (Attachment F) within thirty (30) days of the date of the termination of this Agreement to MHCC in accordance with Section 8 of this Agreement.

4.5 The Parties agree to work together in a mutually agreeable fashion to address technical issues that may arise during project implementation and thereafter. Each Party also agrees to notify the other Party as soon as reasonably practicable if a significant technical issue arises.

5. REPORTING AND NOTIFICATION REQUIREMENTS

5.1 Data Recipient shall submit a semi-annual report to MHCC in the form and manner specified by MHCC, which shall include, but not be limited to, a description of the work performed and uses of the Covered Data; approved changes or expansions to the Scope of Work; approved changes to permitted Data Users; approved changes to data access and security methods; and any approved revisions to the data custodian's data management plan; and a summary of analyses, results, reports, publications, or any other work product derived in whole or part from use of the Covered Data.

5.2 Data Recipient agrees to notify MHCC in writing within 24 hours of receiving a request, subpoena, or order for disclosure relating to the Covered Data, whether for a judicial proceeding or matter, an administrative hearing, a request under Maryland's Public Information Act ("PIA") or the federal Freedom of Information Act ("FOIA"), or similar request. Data Recipient shall not disclose the Covered Data without either MHCC's prior written agreement or before affording the MHCC sufficient time to intervene in opposition to such a request, subpoena, or order.

6. BREACH OF AGREEMENT

6.1 Data Recipient shall give MHCC written notice immediately or as soon as reasonably practicable upon having reason to know that a potential or actual Data Breach, as defined in Section 6.2, has occurred.

6.2 "Data Breach" means the unauthorized acquisition, access, use, or disclosure of the Covered Data, or any unsecured PHI that compromises the security or privacy of such information, subject to the statutory exceptions specified at Section 13400 of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") and the regulatory exclusions specified at 45 C.F.R. §164.402 and any future amendments thereto.

6.3 Any breach of security or unauthorized use or disclosure of the Covered Data, including a Data Breach, shall constitute a breach of this Agreement. Any violation of State or federal law with respect to disclosure of the Covered Data, including but not limited to, the MCMRA or the HIPAA Privacy Rule, shall constitute a breach of this Agreement. Notwithstanding the breaches specifically enumerated above, any other failure by Data Recipient to comply with the terms and obligations of this Agreement shall constitute a breach of this Agreement.

6.4 Any alleged failure of MHCC to act upon a notice of a breach of this Agreement does not constitute a waiver of such breach, nor does it constitute a waiver of any subsequent breach(es).

6.5 The Data Recipient shall comply and assist in any audit of compliance with this Agreement if requested by MHCC. In the event that MHCC reasonably believes that the confidentiality of the Covered Data has been breached, MHCC may: investigate the matter, including an on-site inspection for which Data Recipient shall provide access; and require Data Recipient to develop a written plan of correction, acceptable to MHCC, to ameliorate or minimize the damage caused by the breach of confidentiality and to prevent future breaches of data confidentiality.

6.6 In the event of a breach of this Agreement, MHCC may seek all other appropriate remedies available under law, including termination of this Agreement, disqualification of Data Recipient from receiving PHI or PII from MHCC in the future, and referral of any inappropriate use or disclosure to the Consumer Protection Division of the Office of the Attorney General of Maryland, the Maryland State's Attorney Office, or any other appropriate state or federal law enforcement authority.

7. FEES

7.1

7.2. Data Recipient agrees to pay to MHCC a one-time fee in the amount specified in Section 7.1 for use of the Covered Data. Data Recipient shall pay the fee in full to MHCC before any of the Covered Data is released to Data Recipient.

7.3 No reimbursement will be made to either Party by the other Party for expenses related to accessing, maintaining, or upgrading a Party's information technology infrastructure, or for any expenses related to extracting, using, or storing the Covered Data, or for any other expense otherwise arising out of this Agreement.

8. NOTICE

8.1 Any notice given pursuant to this Agreement must be in writing and addressed to:

If to MHCC:
Mahlet Konjit-Solomon,
Chief of APCD Public Report and Data Release
Maryland Health Care Commission
4160 Patterson Ave. Baltimore, MD
21215
Mahlet.Konjit-Solomon@maryland.gov
(410)-764-3779

If to Data Recipient:
Project Manager Name:
Data Recipient Name
Data Recipient Address
Email:
Telephone:

9. GOVERNING LAW AND JURISDICTION

This Agreement shall be construed, interpreted, and enforced according to the laws of the State of Maryland without reference to its conflict of laws principles. Data Recipient acknowledges doing business in Maryland and agrees to submit to the jurisdiction of the courts in Maryland in the event of an action for an alleged breach of this Agreement.

10. EFFECTIVE DATE, AMENDMENTS, MODIFICATIONS, AND TERMINATION

10.1 This Agreement becomes effective on the date of its execution and shall remain in effect for a period of one (1) year from the date this Agreement is executed, or upon termination of the Agreement by either Party in accordance with section 10.3 below.

10.2 This Agreement may be amended or modified if mutually agreed to in writing by the Parties.

10.3 This Agreement may be terminated by either Party, with or without cause, provided that written notice is given to the non-terminating Party at least thirty (30) days before the determined termination date.

In acknowledgment of the foregoing, the Parties by their duly authorized officials do hereby indicate their consent to this Data Use Agreement.

Maryland Health Care Commission

Signed:

Ben Steffen

Executive Director
Date:

Data Recipient Name

Signed:

Printed Name:

Title
Date:

ATTACHMENT A – Covered Data

This Agreement pertains to the following MCDB data files for the calendar years listed below:

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Pharmacy Claims Files											
Eligibility Claims Files											
Professional Health Claims Files											
Institutional Claims Files											

ATTACHMENT B – Scope of Work

ATTACHMENT C – Additional Data Sources

ATTACHMENT D – Data Users Log

DATE OF LAST UPDATE: _______________________

Data Recipient shall keep a log of the identity of each individual who is authorized to access the data provided under this Agreement. This Attachment contains the log of authorized data users known to Data Recipient at the time of execution of this Agreement. After execution of this Agreement, Data Recipient shall provide written updates of this log to MHCC before authorizing any new individual to access the Covered Data.

By signing my name below as a Data User, I certify that I have reviewed this *DATA USE AGREEMENT BETWEEN THE MARYLAND HEALTH CARE COMMISSION AND* ____.

I understand the confidential nature of the Covered Data and I agree to abide by the required safeguards to protect the security of the data. I understand that the Covered Data can only be used for “Permitted Uses” identified in section 2 of this Agreement and can only be shared with individuals listed and approved in this Data Users Log.

Data Recipient Team:

Name of Data User	Title	Unit	Signature	Date

______________________Team:

Name of Data User	Title	Unit	Signature	Date

____________________**Team:**

Name of Data User	Title	Unit	Signature	Date

________________________**Team:**

Name of Data User	Title	Unit	Signature	Date

ATTACHMENT E – Data Management Plans and Data Storage Locations

ATTACHMENT E: Data Management Plan for ____________________

DATA MANAGEMENT PLAN

Certification

The undersigned certifies and agrees as follows:

- The data will be used only for approved purposes of analysis and presentation.
- The Organization will comply with all administrative, technical, and procedural policies and physical safeguards established to protect the confidentiality of the data and to prevent unauthorized access to the data.
- The data will be encrypted at rest and on motion on storage media (backup tapes, local hard drives, network storage, et al.) with at least an AES-256 standard or stronger.
- The Organization understands and agrees that any intentional breach of confidentiality will result in termination of the Data Use Agreement.
- Anti-virus software or service is active on any server or endpoint containing the MCDB data.
- Staff with access to PHI or other sensitive data have received all relevant training The Organization has policies and procedures in place to address:

- The sharing, transmission, and distribution of PHI
- The physical possession and storage of PHI
- The destruction of PHI upon completion of data use
- Confidentiality agreements with each individuals, including contractors, who will access PHI
- Agreements governing the use and disclosure of PHI with all non-employees who will access PHI

□ Confirm you certify and agree to the above statement

1. Responsible Individuals

a. Provide the name(s) of custodian responsible for receiving, organizing, storing, or archiving data.

Name					
E-Mail Address					
Telephone Number					
Organization Name					
Mailing Address					
City/Town	Columbia	State		Zip Code	

b. Provide the name of the person who will notify MHCC of any breach of the MCDB data, Data Use Agreement or the Data Management Plan.

Name					
E-Mail Address					
Telephone Number					
Organization Name					
Mailing Address					
City/Town	Columbia	State		Zip Code	

c. Provide the name of the person responsible for ensuring proper data destruction upon the termination of the Data Use Agreement, and submission of the Certification of Data Destruction.

Name					
E-Mail Address					
Telephone Number					
Organization Name					
Mailing Address					
City/Town	Columbia	State		Zip Code	

d. Provide the name of the person who will notify MHCC of any project staffing changes, maintain the roster of staff who have formal, documented permission to access specific files for specific purposes, and ensure that all individuals with access to the data comply with the Data Use Agreement.

Name					
E-Mail Address					
Telephone Number					
Organization Name					
Mailing Address					
City/Town		State		Zip Code	

2. Physical Possession and Storage of Data Files

1. List how the data will be stored.

□ Cloud □ Physical Location(s) □ Both

2. Provide the delivery address for the data, including the location where the data will be stored.

i. Delivery Address

Delivery Address			
Address			
City/Town			
State		Zip	

ii. Storage Address

Storage Address			
Address			
City/Town			
State		Zip	

4. Describe the name and data security assessment level of each physical location and the Cloud Service Provider where the data will be stored. Provide evidence that the proposed computing environment meets or exceeds NIST 800-53v4 security standards. Identify all certifications held by entities that will store or hold data.

a) SOC 2 Type Audit
b) HITRUST Certification
c) ISO 27001 Audit Certification
d) Independent external HIPAA standards Assessment
e) SSAE 16 Overview, and/or
f) FedRAMP Certification

5. Has each individual who will access the data agreed to the Request Organization's privacy and security rules when using MCDB data files? ☐ Yes ☐ No

6. Within the last 12 months, has each individual who will access MCDB data received training on the proper handling of protected health information and/or personal data? ☐ Yes ☐ No. If no provide a brief description of the circumstances and detail the training that each such person will receive and by what date.

7. Explain the infrastructure (facilities, hardware, software, etc.) that will secure the MCDB data files.

8. Briefly describe the policies and procedures regarding the physical possession and storage of MCDB data files.

9. Briefly describe the system or the process to track the status and roles of the individuals with access to the MCDB data

10. Briefly describe physical and technical safeguards that will be used to protect MCDB data files.

11. Briefly describe how the data will be backed up and how back up files will be managed.

3. Data Sharing, Electronic Transmission, and Distribution

1. Briefly describe the Requesting Organization's policies and procedures regarding the sharing, transmission, and distribution of sensitive data files (including Data Sharing Agreements).

2. Describe the Requesting Organization's policies and procedures be applicable to the physical removal, transport, and transmission of MCDB data files

3. By checking the boxes next to the following statements, you are confirming that the following requirements will be met.

□ Access to the data will be restricted to authorized users by requiring computer log-on with unique user accounts and passwords.

For data stored on a network drive and not on your computer hard drive:

□ Access will be restricted by limiting folder access to approved study staff only.

□ Any data included in the network backup will be encrypted.

For data stored on the local hard drive of a computer:

□ When not in use, the computer will be locked in a physically secured office, drawer, cabinet or other container to which access is restricted to authorized personnel

□ When not in use, data will be encrypted with a key length of at least 256 bits

4. Describe the Requesting Organization's technical safeguards for data access place:

Password protocols:

Log-on/log-off protocols

Session time out protocols

Encryption for data in motion and data at rest

Antivirus and anti-malware products

5. If applicable, describe the Requesting Organization's physical safeguards for data access and check all security features listed below that are present in the room containing MCDB data files:

□ Recorded video

□ Access log of all individuals entering the room

□ Secure server rack

□ Access control limiting access only to authorized individuals

6. If applicable, identify the data transmission method(s) you plan to use.

□ VPN
□ Secure FTP

□ Encrypted email delivery system
□ Other, please specify and identify why this meets minimum data security requirements below:

7. Describe the Requesting Organization's policies and procedures to protect sensitive data files when individual staff members of project teams (including additional collaborating organizations) terminate their participation on a project. (May

.

4. Completion of Research Tasks and Data Destruction

Applicant must fulfill the requirements of the data request in accordance with the terms and conditions of the Data Use Agreement. All data destruction must follow and conform to NIST SpecialPublications800-88,GuidelinesforMedia Sanitization.

1. Describe the Requesting Organization's process to complete the Certificate of Data Destruction form and the Requesting Organization's policies and procedures to destroy data files upon completion.

2. If a copy of the data is needed to be maintained for a longer period, please provide the reason a longer time period is necessary.

ATTACHMENT F – Certificate of Data Destruction

CERTIFICATE OF DATA DESTRUCTION

Data must be destroyed so that it cannot be recovered from electronic storage media in accordance with the methods established by the "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," as established by the U.S. Department of Health and Human Services (HHS).

The undersigned hereby certifies that all copies of the following data files provided to Data Recipient by

the Maryland Health Care Commission on _________ have been destroyed.

Description of files destroyed (file names provided by MHCC):

Describe how the Data Custodian, System Owner/Maintainer has disposed of, destroyed, erased, and/or anonymized the file regardless of the method of storage. Use as much space as needed to provide a complete description.

Method of destruction:_____________________________________

Date of destruction: _
____

I/we certify that we have destroyed all Data received from MHCC in connection with this project, in all media that were used during the research project. This includes, but is not limited to data maintained on hard drive(s), diskettes, CDs, etc.

SIGNATURES:

Principal Investigator	**Data Custodian**
Organization	Organization
Signature	Signature
Printed Name	Printed Name

Title	Title
Date	Date

Person Responsible for Destroying the Data	**Witness**
Organization	Organization
Signature	Signature
Printed Name	Printed Name
Title	Title
Date	Date

MARYLAND
Health Care
Commission

MD APCD DATA RELEASE ADVISORY COMMITTEE (DRAC)
REVIEW REQUIREMENTS GUIDE

DRAC Responsibilities for Application Review		
1	Criteria for Approval	COMAR 10.25.05.09C
2	Criteria for Disapproval	COMAR 10.25.05.09D
3	Recusal	COMAR 10.25.05.09E
4	External Opinion	COMAR 10.25.05.09F
5	IRB Review	COMAR 10.25.05.09G
6	Request for additional information	COMAR 10.25.05.09H
7	Request for meeting	COMAR 10.25.05.09I
8	Public Comment Reviewed	COMAR 10.25.05.09J

ID #	CRITERIA FOR APPROVAL (COMAR 10.25.05.09C)	Met? (Y/N)
1	Has the applicant provided documentation of relevant education, training, and experience that demonstrates the applicant is capable of undertaking and accomplishing the objective of the proposed use of the data and being a responsible steward of the requested data?	
2	Are the data elements requested by an applicant the minimum amount necessary to achieve the intended purpose for which the data is requested?	
3	Does the proposed use of the data comply with applicable State and federal laws, including those laws relating to the privacy and security of protected health information?	
4	Has the applicant provided a written data management plan that demonstrates appropriate privacy and security controls for access and storage of the data and for safeguarding individual privacy and preventing unauthorized access and use of the data?	
5	Can the requirement of obtaining written authorization from each individual who is the subject of requested identifiable data be waived in accordance with 45 CFR § 164.512?	
PROPOSED LINKAGES		
6	If the applicant has proposed linkage of the requested data to other data source(s), has the applicant has provided:	
6a	Sufficient written justification of the need to link the requested data to the other data source(s) named in the application to accomplish the objective and achieve the results of the proposed use of the data; and	
6b	Written proof that an additional level of data privacy and security controls will be in place to protect the privacy and identification of the individuals who are the subject of the requested data and the other data source(s) to which the requested data is to be linked.	
PUBLIC INTEREST		

7	If an applicant proposes to develop and sell a product that contains de-identified data, has the applicant provided satisfactory written justification of how the proposed sale of the product using the de-identified data will serve the public interest?	
8	Is the proposed use of the data in the public interest?	

ID #	CRITERIA FOR DISAPPROVAL (COMAR 10.25.05.09D)	Does the Application demonstrate any of the following criteria for disapproval? (Y/N)
1	The proposed use of the data violates State or federal law.	
2	The proposed use of the data is not in the public interest.	
3	The proposed use of the data is designed so that the stated objective of the project cannot be met.	
4	False information or documentation on, or related to, the application was provided to Commission staff, the DRAC, the Executive Director, or the Commission.	
5	The applicant provided incomplete information upon which to base a decision on the application.	
6	The applicant or any person or entity that is an officer, owner, operator, or part of management of an applicant's organization who will have access and use of the requested data is not currently, or has not been within ten (10) years prior to the date of the application, a subject of, or a party to a state or federal regulatory agency action or civil or criminal action involving a data breach, HIPAA violation or other matter involving unauthorized access, use, and disclosure of data regardless of whether there has been a finding or admission of guilt, including being:	
6a	Convicted of a felony or pleading guilty, nolo contendere, entering a best interest plea of guilty, or receiving a diversionary disposition regarding a felony;	
6b	A subject of an investigation conducted by, or a pending complaint, charges, or indictment issued by a local, state, or federal governmental regulatory agency or other state or federal law enforcement agency; or	
6c	A party to a final dispositive action in a state or federal governmental agency regulatory action or a civil action that resulted in entry into a settlement agreement, consent agreement, decree, or order, a corporate integrity agreement, corrective action agreement, or other similar agreement or other disposition in a civil action regardless of whether there has been an admission or finding of guilt or liability.	
7	The applicant violated a previous data use agreement.	

8	The data management plan does not demonstrate privacy and security controls for safeguarding individual privacy and preventing unauthorized access to or use of the data.	
9	The proposed use of the data is for an impermissible purpose.	
10	The applicant who proposes to develop and sell a product that contains requested de-identified data has not provided satisfactory written justification of how the proposed sale of the product using the de-identified data will serve the public interest.	